#2

R E P U B L I Q U E F R A N

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 23 JAN. 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA RÈGLE 17.1.a) OU b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ
Code de la propriété intellectuelle - Livre VI

N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire — DB 540 W /260899

Réservé à l'INPI

REMISE DES PIÈCES
DATE 24 DEC. 2002
LIEU 99
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0216933
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 24 DEC. 2002

Vos références pour ce dossier *(facultatif)* TRUSB0015

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET MOUTARD
B.P. 513
78005 VERSAILLES CEDEX

Confirmation d'un dépôt par télécopie ☒ N° attribué par l'INPI à la télécopie 0079

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date
ou demande de certificat d'utilité initiale	N° Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE DE SECURISATION DES SYSTEMES INFORMATIQUES PAR CONFINEMENT LOGICIEL.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	Pays ou organisation Date N° Pays ou organisation Date N° Pays ou organisation Date N° ☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**
5 DEMANDEUR	☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»**
Nom ou dénomination sociale	TRUSTED LOGIC
Prénoms	
Forme juridique	société anonyme
N° SIREN	4 2 1 4 8 3 4 1 3
Code APE-NAF	7 2 1 Z
Adresse — Rue	5, rue du Bailliage
Adresse — Code postal et ville	78000 VERSAILLES
Pays	France
Nationalité	française
N° de téléphone *(facultatif)*	
N° de télécopie *(facultatif)*	
Adresse électronique *(facultatif)*	

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES
DATE
LIEU 99 24 DEC. 2002
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0216933

DB 540 W /260899

Vos références pour ce dossier : *(facultatif)*		TRUSB0015
6 **MANDATAIRE**		
Nom		de Saint Palais
Prénom		Arnaud
Cabinet ou Société		CABINET MOUTARD
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	35, rue de la Paroisse
	Code postal et ville	78000 VERSAILLES
N° de téléphone *(facultatif)*		01 30 83 79 79
N° de télécopie *(facultatif)*		01 30 83 79 78
Adresse électronique *(facultatif)*		asp@moutard.fr
7 **INVENTEUR (S)**		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 **RAPPORT DE RECHERCHE**		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en trois versements, uniquement pour les personnes physiques** ☐ Oui ☐ Non
9 **RÉDUCTION DU TAUX DES REDEVANCES**		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :*
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 **SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)** A. de Saint Palais - No 94-0306	**VISA DE LA PRÉFECTURE OU DE L'INPI** M. MARTIN

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

La présente invention concerne la sécurisation des systèmes informatiques par confinement logique de données.

Elle a plus particulièrement pour objet la sécurisation des systèmes informatiques offrant la possibilité d'exécution de codes manipulant des données qui doivent être traitées séparément. Cette séparation est généralement dictée par des besoins de sécurité. A titre d'exemple, les données du système d'exploitation qui conditionnent le bon fonctionnement de la plate-forme ne doivent pas pouvoir être modifiées par une application quelconque. De même, dans les systèmes permettant l'exécution d'applications multiples, les données d'une application doivent généralement être protégées des autres applications.

Ces besoins prennent dans certains cas un caractère critique ; on peut penser par exemple, et de manière non limitative, aux systèmes embarqués multi-applicatifs du type cartes à puce, terminaux de paiement, assistants digitaux, ou téléphones portatifs, surtout lorsque ces systèmes embarqués permettent le télé-chargement d'applications. En effet, ces applications téléchargées peuvent provenir de sites multiples, qui offrent des garanties de confiance très variées.

BEST AVAILABLE COPY

D'une façon générale, on sait que la plupart des solutions généralement adoptées pour répondre à ce besoin de séparation desdites données de systèmes d'exploitation et d'applications repose sur l'utilisation de mécanismes proposés par le matériel. Typiquement, des unités (physiques) de gestion de mémoire ("MMU, ou Memory Management Unit") associent des espaces physiques à des applications et les protègent contre des accès provenant d'autres applications. Cependant, cette solution, quand elle est disponible, n'est pas très souple et s'associe difficilement aux systèmes d'allocation dynamique de données (le nombre d'espaces physiques étant fixe), spécialement dans le cas des systèmes embarqués disposant de peu de ressources et soumis à de fortes contraintes de sécurité.

La présente invention a donc plus particulièrement pour but de palier à ces inconvénients.

Elle propose, à cet effet, de rendre plus flexible la sécurisation des données et de l'étendre au cas d'allocation dynamique de mémoire.

Elle fait essentiellement intervenir :

- au moins un gestionnaire de mémoire gérant des unités d'allocation mémoire qui peuvent être typiquement une page de taille fixe ou un bloc de taille variable,
- au moins des possesseurs et des demandeurs d'allocation mémoire pouvant être typiquement des applications de l'utilisateur du système d'exploitation du système informatique ou le système d'exploitation lui-même.

Selon l'invention, le procédé de sécurisation d'un système informatique par confinement logique de données comprend la séparation desdites données par possesseur et leur chiffrement avec une clé dédiée ; ce processus de

séparation et de chiffrement s'effectue grâce à un mode opératoire comprenant les étapes suivantes :

- une allocation de mémoire réalisée par un gestionnaire de mémoire à la demande d'un autre composant du système d'exploitation qui transmet audit gestionnaire de mémoire l'identité du demandeur. Ce demandeur deviendra le possesseur de la mémoire allouée. La transmission de l'identité du demandeur peut se faire soit par la gestion d'un contexte courant, soit par le passage de paramètres aux fonctions du gestionnaire de mémoire ;
- un contrôle par le susdit gestionnaire de mémoire de l'ensemble des unités d'allocation mémoire, chacune étant associée à un possesseur de l'unité d'allocation mémoire. Chaque unité d'allocation mémoire ne peut avoir qu'un et un seul possesseur ; néanmoins plusieurs unités d'allocation mémoire peuvent avoir le même possesseur ;
- une utilisation par le gestionnaire de mémoire d'un secret associé à chaque possesseur. Ce secret peut typiquement être fourni au gestionnaire de mémoire par le système d'exploitation au moment de l'introduction du possesseur dans le système ou à chaque accès à une unité d'allocation mémoire ;
- une utilisation par le gestionnaire de mémoire d'une clé pour chaque possesseur. Cette clé peut par exemple être dérivée d'un secret associé au possesseur et une clé dite "maître" à laquelle seul le gestionnaire de mémoire a accès ;
- une vérification par le gestionnaire de mémoire, pour chaque demande d'accès à une unité d'allocation mémoire, de l'identité du demandeur ; si cette identité n'est pas identique à celle du possesseur de ladite unité d'allocation mémoire, alors l'accès à l'unité d'allocation mémoire est refusé par le gestionnaire de mémoire ;
- une réalisation par le gestionnaire de mémoire du chiffrement (dans le cas d'une demande d'écriture) ou du déchiffrement (dans le cas d'une demande

de lecture) des données concernées avec la clé associée au possesseur, cette clé pouvant être recalculée par le gestionnaire de mémoire.

Ainsi, les données des différents possesseurs étant chiffrées de manière automatique, par un secret que seul le gestionnaire de mémoire connaît, il est impossible pour une application d'avoir accès aux données d'un autre possesseur.

Deux situations peuvent se présenter lorsqu'un tiers tente d'accéder à une unité d'allocation mémoire qui ne lui appartient pas :

- cette tentative peut être déclenchée par l'intermédiaire du gestionnaire de mémoire : dans ce cas, le contrôle effectué par le gestionnaire de mémoire conduit automatiquement au rejet de la demande ;
- cette tentative peut être déclenchée de manière illicite, sans passer par l'intermédiaire du gestionnaire de mémoire, par accès direct à la mémoire physique, dans le cas où les vérifications effectuées par le matériel ne suffisent pas à écarter cette possibilité : le tiers pourra alors effectuer une lecture, mais, ne disposant pas de la clé de déchiffrement, il obtiendra des données inutilisables.

A partir du moment où la clé maître est mémorisée dans une zone protégée, la confidentialité des données est donc préservée dans les deux cas.

Avantageusement, le procédé selon l'invention ne dépend pas du fait que l'unité d'allocation mémoire soit une page logique de taille fixe ou un bloc de taille variable. Dans le cas où l'unité d'allocation est la page, le procédé se raffinera de la façon suivante : lorsque le gestionnaire de mémoire reçoit une demande d'allocation d'un bloc pour le compte d'un possesseur, il recherche d'abord une page ayant le même possesseur ; ainsi, tous les blocs alloués par un possesseur d'unité d'allocation mémoire se trouvent regroupés dans une ou plusieurs pages dédiées.

Le procédé selon l'invention pourra être amélioré de plusieurs manières (non exclusives) :

- Au lieu d'associer une clé unique à un possesseur donné, le gestionnaire de mémoire peut associer une clé à chaque ensemble possesseur et unité d'allocation mémoire. Cette amélioration a deux avantages : d'une part, elle réduit les probabilités de découverte des clés utilisées (en cas d'attaque cryptographique) puisque chaque clé sera utilisée moins souvent ; d'autre part, elle réduit les risques en cas de découverte d'une clé puisque seule l'unité d'allocation mémoire associée sera mise en danger.

- Le gestionnaire de mémoire peut également intégrer dans chaque unité de mémoire une zone permettant d'en vérifier l'intégrité, par exemple à partir d'un simple "checksum" (somme des contrôles) signé ou d'un algorithme cryptographique. La donnée contenue dans cette zone est mise à jour par le gestionnaire de mémoire à chaque accès en écriture à l'unité. Elle peut être utilisée par le gestionnaire de mémoire à des fins de vérification, soit systématiquement à chaque accès à l'unité, soit de façon périodique. La vérification consiste simplement, avant l'accès demandé, à recalculer la donnée d'intégrité à partir du contenu de l'unité (données en clair) et à la comparer à la donnée contenue dans la zone d'intégrité. Une modification intempestive ou illicite du contenu de l'unité pourra alors être détectée, ce qui renforcera la sécurité de la gestion des données.

- L'association de différents niveaux de sécurité aux applications et l'utilisation de moyens de chiffrement différents (typiquement algorithmes, longueurs de clés) selon le niveau de sécurité associé permettent de proportionner le coût de mise en oeuvre (temps d'exécution notamment) à l'objectif recherché en matière de sécurité.

A titre d'exemple non limitatif, il pourra être justifié de réserver les moyens cryptographiques les plus puissants (et les plus coûteux) pour la protection d'une unité de mémoire destinée à recevoir des clefs de chiffrement ou des droits d'accès.

- La combinaison du procédé selon l'invention à un mécanisme de protection physique (MMU) permet une protection à granularité plus fine. Par exemple, les applications peuvent être regroupées en plusieurs grandes catégories (éventuellement, et de manière non limitative, selon le niveau de confiance qu'on peut leur accorder, la première distinction naturelle pouvant être entre applications des utilisateurs et applications du système d'exploitation), chaque catégorie étant protégée des autres par le mécanisme physique et les applications étant protégées entre elles par le procédé de confinement logiciel selon l'invention.

REVENDICATIONS

1. Procédé de sécurisation par confinement logiciel d'un système informatique qui exécute des codes manipulant des données, faisant intervenir :

- au moins un gestionnaire de mémoire gérant des unités d'allocation mémoire qui peuvent être typiquement une page de taille fixe ou un bloc de taille variable,
- au moins des possesseurs et des demandeurs d'unités d'allocation mémoire pouvant être typiquement une application de l'utilisateur du système d'exploitation du système informatique ou le système d'exploitation lui-même,

caractérisé en ce qu'il comprend une séparation des données par possesseur d'au moins une unité d'allocation mémoire et le chiffrement desdites données avec une clé dédiée.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comprend les étapes suivantes :

- une allocation de mémoire réalisée par le gestionnaire de mémoire à la demande d'un autre composant du système d'exploitation qui transmet audit gestionnaire de mémoire l'identité du demandeur ;
- un contrôle par le susdit gestionnaire de mémoire de l'ensemble des unités d'allocation, chacune étant associée à un possesseur de l'unité d'allocation mémoire ;
- une utilisation par le gestionnaire de mémoire d'un secret associé à chaque possesseur ;
- une utilisation par le gestionnaire de mémoire d'une clé pour chaque possesseur ;
- une vérification par le gestionnaire de mémoire, pour chaque demande d'accès à une unité d'allocation mémoire, de l'identité du demandeur ; si cette identité n'est pas identique à celle du possesseur de ladite unité

d'allocation mémoire, alors l'accès à l'unité d'allocation mémoire est refusé par le gestionnaire de mémoire ;

- une réalisation par le gestionnaire de mémoire du chiffrement (dans le cas d'une demande d'écriture) ou du déchiffrement (dans le cas d'une demande de lecture) des données concernées avec la clé associée au possesseur, cette clé étant au moins recalculée par le gestionnaire de mémoire.

3. Procédé selon la revendication 2, caractérisé en ce que l'unité d'allocation est la page, et que le gestionnaire de mémoire, lorsqu'il reçoit une demande d'allocation d'un bloc pour le compte d'un possesseur d'unité d'allocation mémoire, recherche d'abord une page ayant le même possesseur de façon à ce que tous les blocs alloués par ledit possesseur se trouvent regroupés dans une ou plusieurs pages dédiées.

4. Procédé selon la revendication 2, caractérisé en ce que la transmission de l'identité du demandeur se fait soit par la gestion d'un contexte courant, soit par le passage de paramètres aux fonctions du gestionnaire de mémoire.

5. Procédé selon la revendication 2, caractérisé en ce que le gestionnaire de mémoire calcul dynamiquement la clé d'un possesseur à partir du secret associé audit possesseur et d'une clé dite "maître" à laquelle seule le gestionnaire de mémoire a accès.

6. Procédé selon la revendication 1, caractérisé en ce que le gestionnaire de mémoire associe une clé à chaque ensemble possesseur et unité d'allocation mémoire au lieu d'associer une clé unique à chaque possesseur.

7. Procédé selon la revendication 1, caractérisé en ce que le gestionnaire de mémoire intègre dans chaque unité d'allocation mémoire une zone permettant d'en vérifier l'intégrité.

8. Procédé selon la revendication 1, caractérisé en ce qu'il associe différents niveaux de sécurité aux applications et utilise des moyens de chiffrement différents selon le niveau de sécurité associé.

9. Procédé selon la revendication 1, caractérisé en ce qu'il est combiné à un mécanisme de protection physique.

10. Procédé selon la revendication 1, caractérisé en ce qu'il est implémenté sur un système embarqué tel un terminal du type téléphone portatif, un terminal de paiement bancaire, un terminal de paiement portatif, un assistant digital ou "PDA", une carte à puce.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11 235*02

DÉPARTEMENT DES BREVETS
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W /260899

Vos références pour ce dossier *(facultatif)*	TRUSB0015
N° D'ENREGISTREMENT NATIONAL	02 16933 du 24 décembre 2002

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE DE SECURISATION DES SYSTEMES INFORMATIQUES PAR CONFINEMENT LOGICIEL.

LE(S) DEMANDEUR(S) :

CABINET MOUTARD - 35, rue de la Paroisse - 78000 VERSAILLES - agissant en qualité de mandataire auprès de :
TRUSTED LOGIC (société anonyme)
5, rue du Bailliage
78000 VERSAILLES

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		HAMEAU	
Prénoms		Patrice	
Adresse	Rue	18, rue de Belle-Feuille	
	Code postal et ville	92100	BOULOGNE BILLANCOURT
Société d'appartenance *(facultatif)*			
Nom		LE METAYER	
Prénoms		Daniel	
Adresse	Rue	23, rue de la Celle	
	Code postal et ville	78150	LE CHESNAY
Société d'appartenance *(facultatif)*			
Nom		MESNIL	
Prénoms		Cédric	
Adresse	Rue	25, avenue du Val d'Arcy	
	Code postal et ville	78340	LES CLAYES SOUS BOIS
Société d'appartenance *(facultatif)*			

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

03 janvier 2003

A. de Saint Palais - No 94-0306

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.